Listing of the Claims:

1-30. (Cancelled)

31. (Previously Presented) A method for conducting a transaction between a first computer system and a second computer system, the method comprising the steps of:

(a) receiving in the second computer system a request from a user of the first computer system to download data from the second computer system;

(b) determining by the second computer system whether the request represents a new transaction or an incomplete transaction by comparing a first value stored in the first computer system with a second value stored in the second system; and

(c) if the request represents an incomplete transaction, completing the transaction, wherein the user is not charged duplicate fees associated with starting a new transaction.

32. (Previously Presented) The method of claim 31 wherein the first system comprises a client system and the second system comprises a server system.

33. (Previously Presented) The method of claim 32 wherein the first value of the client system is stored in a persistent client-side data file.

34. (Previously Presented) The method of claim 33 wherein the persistent client-side data file comprises a cookie.

35. (Previously Presented) The method of claim 34 wherein step b) further comprises:

b1) allowing the server system to compare the first value in the cookie with the second value in the server system.

36. (Previously Presented) The method of claim 31, wherein the request represents a new transaction if the first value does not match a part of the second value, the method further comprising:

d) if the request represents a new transaction, generating a new encryption key by the second system, wherein the new encryption key is associated with the new transaction;

e) storing a first portion of the new encryption key in the first computer system as the first value; and

f) storing the whole new encryption key on the second computer system as the second value.

37. (Previously Presented) The method of claim 36 further comprising:

g) encrypting the requested data with the whole new encryption key;

h) transmitting the encrypted data from the second computer system to the first computer system; and

i) after the encrypted data has been transmitted, sending a remaining portion of the new encryption key from the second computer system to the first computer system,

wherein the first computer system combines the first portion and the remaining portion of the new encryption key to form the whole new encryption key and utilizes the whole new encryption key to decrypt the encrypted data.

38. (Previously Presented) The method of claim 37 further comprising:

j) after the encrypted data has been transmitted and prior to sending the remaining portion of the new encryption key, allowing the user to provide payment for the whole new encryption key.

39. (Previously Presented) The method of claim 31, wherein the first value is a first portion of an encryption key and the second value is a whole encryption key, and step c) further comprises:

c1) encrypting the requested data with the whole encryption key;

c2) transmitting the encrypted data from the second computer system to the first computer system; and

c3) after the encrypted data has been transmitted, sending a remaining portion of the encryption key from the second computer system to the first computer system, whereby the first computer system combines the first portion and the remaining portion of the encryption key to form the whole encryption key and utilizes the whole encryption key to decrypt the encrypted data.

40. (Previously Presented) The method of claim 39, wherein step (c) further comprises:

c4) after the encrypted data has been transmitted and prior to sending the remaining portion of the encryption key, allowing the user to provide payment for the whole encryption key. .

41. (Previously Presented) A system for conducting a transaction between a first computer system and a second computer system, the system comprising:

means in the second computer system for receiving a request from a user of the first computer system to download data from the second computer system;

means for determining by the second computer system whether the request represents a new transaction or an incomplete transaction by comparing a first value stored in the first computer system with a second value stored in the second system; and

means for completing the incomplete transaction if the request represents an incomplete transaction,

wherein the user is not charged duplicate fees associated with starting a new transaction.

42. (Previously Presented) The system of claim 41 wherein the first system comprises a client system and the second system comprises a server system.

43. (Previously Presented) The system of claim 42 wherein the first value of the client system is stored in a persistent client-side data file.

44. (Previously Presented) The system of claim 43 wherein the persistent client-side data file comprises a cookie.

45. (Previously Presented) The system of claim 44 wherein the means for determining further comprises:

means for allowing the server system to compare the first value in the cookie with the second value in the server system.

46. (Previously Presented) The system of claim 41 wherein the request represents a

new transaction if the first value does not match a part of the second value and wherein the system further comprises:

means in the second system for generating a new encryption key, wherein the new encryption key is associated with the new transaction;

means in the second system for storing a first portion of the new encryption key in the first computer system as the first value; and

means in the second system for storing the whole new encryption key on the second computer system as the second value.

47. (Previously Presented) The system of claim 46 further comprising:

means for encrypting the requested data with the whole new encryption key;

means in the second computer system for transmitting the encrypted data from the second computer system to the first computer system; and

means in the second computer system for sending a remaining portion of the new encryption key from the second computer system to the first computer system, whereby the first computer system combines the first portion and the remaining portion of the new encryption key to form the whole new encryption key and utilizes the whole new encryption key to decrypt the encrypted data.

48. (Previously Presented) The system of claim 47 further comprising:

means for allowing the user to provide payment for the whole new encryption key after the encrypted data has been transmitted and prior to sending the remaining portion of the new encryption key.

49. (Previously Presented) The system of claim 41, wherein the first value is a first portion of an encryption key and the second value is a whole encryption key, and the means for completing the incomplete transaction comprises:

means for encrypting the requested data with the whole encryption key;

means in the second computer system for transmitting the encrypted data from the second computer system to the first computer system; and

means in the second computer system for sending a remaining portion of the encryption key from the second computer system to the first computer system,

whereby the first computer system combines the first portion and the remaining portion of the encryption key to form the whole encryption key and utilizes the whole encryption key to decrypt the encrypted information.

50. (Previously Presented) The system of claim 49 wherein the means for completing the incomplete transaction further includes means for allowing the user to provide payment for the whole encryption key after the encrypted data has been transmitted and prior to sending the remaining portion of the encryption key.

51. (Previously Presented) A computer readable medium containing program instructions for conducting a transaction between a first computer system and a second computer system, the program instructions for:

(a) receiving in the second computer system a request from a user of the first computer system to download data from the second computer system;

(b) determining by the second computer system whether the request represents a new

transaction or an incomplete transaction by comparing a first value stored in the first computer system with a second value stored in the second system; and

(c) if the request represents an incomplete transaction, completing the transaction, wherein the user is not charged duplicate fees associated with starting a new transaction.

52. (Previously Presented) The computer readable medium of claim 51 wherein the first system comprises a client system and the second system comprises a server system.

53. (Previously Presented) The computer readable medium of claim 52 wherein the first value of the client system is stored in a persistent client-side data file.

54. (Previously Presented) The computer readable medium of claim 53 wherein the persistent client-side data file comprises a cookie.

55. (Previously Presented) The computer readable medium of claim 54 wherein instruction b) further comprises:

b1) allowing the server system to compare the first value in the cookie with the second value in the server system.

56. (Previously Presented) The computer readable medium of claim 51, wherein the request represents a new transaction if the first value does not match a part of the second value, the method further comprising:

d) if the request represents a new transaction, generating a new encryption key by the second system, wherein the new encryption key is associated with the new transaction;

e) storing a first portion of the new encryption key in the first computer system as the first value; and

f) storing the whole new encryption key on the second computer system as the second value.

57. (Previously Presented) The computer readable medium of claim 56 further comprising:

g) encrypting the requested data with the whole new encryption key;

h) transmitting the encrypted data from the second computer system to the first computer system; and

i) after the encrypted data has been transmitted, sending a remaining portion of the new encryption key from the second computer system to the first computer system,

wherein the first computer system combines the first portion and the remaining portion of the new encryption key to form the whole new encryption key and utilizes the whole new encryption key to decrypt the encrypted data.

58. (Previously Presented) The computer readable medium of claim 57 further comprising:

j) after the encrypted data has been transmitted and prior to sending the remaining portion of the new encryption key, allowing the user to provide payment for the whole new encryption key.

59. (Previously Presented) The computer readable medium of claim 51 wherein the first value is a first portion of an encryption key and the second value is a whole encryption key,

and instruction c) further comprises:

c1) encrypting the requested data with the whole encryption key;

c2) transmitting the encrypted data from the second computer system to the first computer system; and

c3) after the encrypted data has been transmitted, sending a remaining portion of the encryption key from the second computer system to the first computer system, whereby the first computer system combines the first portion and the remaining portion of the encryption key to form the whole encryption key and utilizes the whole encryption key to decrypt the encrypted data.

60. (Previously Presented) The computer readable medium of claim 59, wherein instruction (c) further comprises:

c4) after the encrypted data has been transmitted and prior to sending the remaining portion of the encryption key, allowing the user to provide payment for the whole encryption key.

61. (Previously Presented) A method for conducting a transaction between a first computer system and a second computer system, the method comprising the steps of:

(a) receiving in the second computer system a request from a user of the first computer system to download data from the second computer system;

(b) determining by the second computer system whether the request represents a new transaction or an incomplete transaction by comparing a first value stored in the first computer system with a second value stored in the second system; and

(c) if the request represents an incomplete transaction, completing the transaction,

wherein the user is not charged duplicate fees associated with starting a new transaction;

wherein the first value is a first portion of an encryption key and the second value is a whole encryption key, and step c) further comprises:

c1) encrypting the requested data with the whole encryption key;

c2) transmitting the encrypted data from the second computer system to the first computer system; and

c3) after the encrypted data has been transmitted, sending a remaining portion of the encryption key from the second computer system to the first computer system, whereby the first computer system combines the first portion and the remaining portion of the encryption key to form the whole encryption key and utilizes the whole encryption key to decrypt the encrypted data.

62. (Previously Presented) A system for conducting a transaction between a first computer system and a second computer system, the system comprising:

means in the second computer system for receiving a request from a user of the first computer system to download data from the second computer system;

means for determining by the second computer system whether the request represents a new transaction or an incomplete transaction by comparing a first value stored in the first computer system with a second value stored in the second system; and

means for completing the incomplete transaction if the request represents an incomplete transaction,

wherein the user is not charged duplicate fees associated with starting a new transaction;

wherein the first value is a first portion of an encryption key and the second value is a

whole encryption key, and the means for completing the incomplete transaction comprises:

means for encrypting the requested data with the whole encryption key;

means in the second computer system for transmitting the encrypted data from the second computer system to the first computer system; and

means in the second computer system for sending a remaining portion of the encryption key from the second computer system to the first computer system,

whereby the first computer system combines the first portion and the remaining portion of the encryption key to form the whole encryption key and utilizes the whole encryption key to decrypt the encrypted information.

63. (Previously Presented) A computer readable medium containing program instructions for conducting a transaction between a first computer system and a second computer system, the program instructions for:

(a) receiving in the second computer system a request from a user of the first computer system to download data from the second computer system;

(b) determining by the second computer system whether the request represents a new transaction or an incomplete transaction by comparing a first value stored in the first computer system with a second value stored in the second system; and

(c) if the request represents an incomplete transaction, completing the transaction, wherein the user is not charged duplicate fees associated with starting a new transaction;

wherein the first value is a first portion of an encryption key and the second value is a whole encryption key, and instruction c) further comprises:

c1) encrypting the requested data with the whole encryption key;

c2) transmitting the encrypted data from the second computer system to the first computer system; and

c3) after the encrypted data has been transmitted, sending a remaining portion of the encryption key from the second computer system to the first computer system, whereby the first computer system combines the first portion and the remaining portion of the encryption key to form the whole encryption key and utilizes the whole encryption key to decrypt the encrypted data.